UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/564,421	01/11/2006	Antonius Adrianus Kalker	NL 030808	8966

24737 7590 01/21/2009
PHILIPS INTELLECTUAL PROPERTY & STANDARDS
P.O. BOX 3001
BRIARCLIFF MANOR, NY 10510

EXAMINER	
POGMORE, TRAVIS D	

ART UNIT	PAPER NUMBER
4148	

MAIL DATE	DELIVERY MODE
01/21/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/564,421	KALKER ET AL.	
	Examiner	Art Unit	
	Travis Pogmore	2436	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 December 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-3 and 5-15* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3 and 5-15* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to the request for reconsideration filed December 3, 2008.

2. Claims 1-3 and 5-15 are currently pending. Claims 1-3, 6-7, 9, and 14-15 are currently amended; claims 5, 8, and 12-13 have been previously presented and claims 4 and 16 have been cancelled.

3. Applicant's arguments, with regards to claims 1-16, filed December 3, 2008 have been fully considered but they are not persuasive.

Examiner Notes

4. Examiner cites particular columns and line numbers in the references as applied to the claims below for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested that, in preparing responses, the applicant fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the examiner.

5. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claim Objections

6. Applicant's arguments, see page 5, and respective amendments filed December 3, 2008, with respect to the informality of claims 2 have been fully considered and are persuasive. The objection of claim 2 has been withdrawn.

Claim Rejections – 35 USC § 112

7. As claim 16 has been canceled, the rejection thereof has been withdrawn.

Claim Rejections – 35 USC § 101

8. As claim 16 has been canceled, the rejection thereof has been withdrawn.

Claim Rejections – 35 USC § 102

9. Claims 1-3, 5-8 and 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over "Secret key watermarking with changing keys" 10 September 2000, pages 427-429, XP010530642 (hereinafter "Depovere") in view of U.S. Patent Application Pub. No. US 2002/002800 A1 (hereinafter "Conwell") and further in view of U.S. Patent No. 5,724,425 (hereinafter "Chang").

As to claim 1, Depovere teaches a method of embedding a digital watermark in an information signal; the method comprising

deriving a watermark secret (page 427, column 1 and Fig. 1, and page 429, column 1, first paragraph, it is inherent that the detector being able to store the secret key patterns (i.e. watermark secret) means that it must be able to derive the watermark

secret from identifier data, otherwise it would be required to generate them on the fly every time);

embedding a digital watermark in the information signal where said embedding is controlled by the watermark secret (page 427, column 1 and Fig. 1); but does not specifically teach wherein the watermark secret is derived by a function which is computationally hard or infeasible to invert;

calculating a digital fingerprint from the information signal; nor

storing the calculated digital fingerprint as a reference digital fingerprint and storing, in relation to the reference digital fingerprint, said identifier data item.

However, Conwell teaches calculating a digital fingerprint from the information signal (page 1, column 1, paragraph 9 and column 2, paragraphs 18-19); and

storing the calculated digital fingerprint as a reference digital fingerprint and storing, in relation to the reference digital fingerprint, said identifier data item (page 2, column 1, paragraphs 23 and 25, the database stores the one or more songs (e.g. a song title being the identifier data item) which match the fingerprint in the database (i.e. is stored in relation to the fingerprint)), but does not specifically teach wherein the watermark secret is derived from an identifier data item identifying the information signal by a function which is computationally hard or infeasible to invert.

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Depovere to fingerprint the information signal and store it along with an identifier as in Conwell because this would allow

decreased complexity of watermark detection (Depovere, page 429, column 1, first paragraph).

Furthermore, Chang teaches wherein the watermark secret is derived from an identifier data item identifying the information signal by a function which is computationally hard or infeasible to invert is well known and expected in the art (column 18, line 59 to column 19, line 3, where the two numbers P and Q comprise or are otherwise related to the identifier data item and the secret is the calculated value N).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Depovere to relate the watermark secret to the identifiers with a function that is computationally infeasible to invert as in Chang because this makes the secret (and thus the watermark) cryptographically secure.

As to claim 2, Conwell teaches wherein the information signal is an audio signal (Abstract), the digital fingerprint is an audio fingerprint (Abstract), and the digital watermark is an audio watermark (page 2, column 2, paragraph 35).

As to claim 3, Conwell teaches wherein storing the calculated digital fingerprint and said identifier data item comprises storing the calculated digital fingerprint and the identifier data item in a fingerprint database (page 1, column 1, paragraph 9).

As to claim 5, Depovere and Conwell teach a method according to claim 1, but do not specifically teach wherein the watermark secret is determined by a random process.

However, Chang teaches that wherein the watermark secret is determined by a random process is well known and expected in the art (column 18, lines 62-65, since the secret is the two numbers P and Q and they are chosen at random, the secret as a whole is determined at random).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Depovere and Conwell to determine the watermark secret by a random process as in Chang because this makes the fingerprint more cryptographically secure.

As to claim 6, Conwell teaches where the digital watermark comprises a watermark payload (page 2, column 2, paragraph 35 to page 3, column 1, paragraph 36) and wherein the watermark payload is indicative of the information signal (page 2, column 2, paragraph 35, since the fingerprint is calculated from the information signal if it is placed in the payload then the payload is indicative of the information signal).

As to claim 7, Depovere teaches further comprising deriving an encryption key from an identifier indicative of an information content of the information signal (page 428, column 2, section 3, a "robust signature" (i.e. identifier) as recited is created by combining features (i.e. information content) of the information signal, and is associated

with one of the "secret keys" (i.e. an encryption key)), but does not specifically teach encoding said watermark payload based on an encryption key.

However Conwell teaches encoding said watermark payload based on an encryption key (page 3, column 1, paragraph 38, specifically lines 6-8)

As to claim 8, Conwell teaches wherein the information signal is a video signal (page 4, column 2, paragraph 57).

As to claim 14, Depovere teaches an arrangement for embedding a digital watermark in an information signal; the arrangement comprising

- means for deriving a watermark secret (page 427, column 1 and Fig. 1, and page 429, column 1, first paragraph, it is inherent that the detector being able to store the secret key patterns (i.e. watermark secret) means that it must be able to derive the watermark secret from identifier data, otherwise it would be required to generate them on the fly every time);

- means for embedding a digital watermark in an information signal where said embedding is controlled by a watermark secret (page 427, column 1 and Fig. 1); but does not specifically teach wherein the watermark secret is derived from an identifier data item identifying the information signal by a function which is computationally hard or infeasible to invert;

- means for calculating a digital fingerprint from the information signal; nor

- means for storing the calculated digital fingerprint as a reference digital fingerprint and for storing, in relation to the reference digital fingerprint, a identifier data item from which the watermark secret can be derived.

However, Conwell teaches a means for calculating a digital fingerprint from the information signal (page 1, column 1, paragraph 9 and column 2, paragraphs 18-19); and

- means for storing the calculated digital fingerprint as a reference digital fingerprint and for storing, in relation to the reference digital fingerprint, a identifier data item from which the watermark secret can be derived (page 2, column 1, paragraphs 23 and 25, the database stores the one or more songs (e.g. a song title being the identifier data item) which match the fingerprint in the database (i.e. is stored in relation to the fingerprint)), but does not specifically teach wherein the watermark secret is derived from an identifier data item identifying the information signal by a function which is computationally hard or infeasible to invert.

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Depovere to fingerprint the information signal and store it along with an identifier as in Conwell because this would allow decreased complexity of watermark detection (Depovere, page 429, column 1, first paragraph).

Furthermore, Chang teaches wherein the watermark secret is derived from an identifier data item identifying the information signal by a function which is computationally hard or infeasible to invert is well known and expected in the art

(column 18, line 59 to column 19, line 3, where the two numbers P and Q comprise or are otherwise related to the identifier data item and the secret is the calculated value N).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Depovere to relate the watermark secret to the identifiers with a function that is computationally infeasible to invert as in Chang because this makes the secret (and thus the watermark) cryptographically secure.

10. Claims 9-13 and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Conwell in view of Depovere.

As to claim 9, Conwell teaches a method of detecting a digital watermark in an information signal; the method comprising

- providing a plurality of digital reference fingerprints each calculated from a respective reference information signal (page 1, column 1, paragraph 9 and page 2, column 1, paragraph 25);

- calculating a digital fingerprint from an information signal (page 1, column 1, paragraph 9 and column 2, paragraphs 18-19); and

- determining a matching digital fingerprint from the plurality of digital reference fingerprints as corresponding to the calculated digital fingerprint (page 2, column 1, paragraph 25); but does not specifically teach where each digital fingerprint is associated with a corresponding watermark secret; or

- detecting whether a digital watermark according to the watermark secret associated with the matching digital fingerprint is present in the information signal.

However, Depovere teaches where each digital fingerprint is associated with a corresponding watermark secret (page 427, column 1 and Fig. 1); and

- detecting whether a digital watermark according to the watermark secret associated with the matching digital fingerprint is present in the information signal (page 427, column 1 and Fig. 1 and page 428, column 2).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Conwell to use a watermark secret as in Depovere because it increases the security of the system (Depovere, page 427, column 2).

As to claim 10, Conwell teaches wherein determining a matching digital fingerprint comprises sending a query to a fingerprint database, the query comprising the calculated digital fingerprint (page 2, column 1, paragraphs 25-26); and receiving from the fingerprint database a response including a identifier data item from which the watermark secret associated with the matching digital fingerprint can be derived (page 1, column 1, paragraph 9).

As to claim 11, Conwell teaches wherein sending a query and receiving a response comprise communicating via a communications network is well known and

expected in the art (page 2, column 2, paragraphs 33-34, in particular the reference to sending a fingerprint to CDDB.com and it returning relevant IDs).

As to claim 12, Conwell teaches wherein the information signal comprises an encoded information signal; and calculating the digital fingerprint comprises decoding the encoded information signal, and calculating the fingerprint from the decoded information signal is well known and expected in the art (page 1, column 1, paragraph 11 to column 2, paragraph 12 and paragraphs 19-20; under the broadest reasonable interpretation of an encoded information signal it is inherent that any information signal that is digital (and thus processable by computer as in paragraphs 11-12) is encoded (i.e. in bits which are specifically determined by bit depth and sample rate); it is also inherent that being able being able to acoustically compare songs sampled at differed bit rates (and thus the bits would not be identical) as in paragraphs 19-20 requires that the songs be decoded to some other form before calculating a fingerprint.

As to claim 13, Conwell teaches wherein determining a matching digital fingerprint comprises performing a search in a fingerprint database based on reliability information about the calculated digital fingerprint (page 2, column 1, paragraphs 26-29 and page 3, column 2, paragraph 42 to page 4, column 1, paragraph 48, a probabilistic method of determining the most likely match for a given fingerprint (or fingerprints) is reliability information).

As to claim 15, Conwell teaches an arrangement for detecting a digital watermark in an information signal; the arrangement comprising

- means for providing a plurality of digital reference fingerprints each calculated from a respective reference information signal (page 1, column 1, paragraph 9 and page 2, column 1, paragraph 25);

- means for calculating a digital fingerprint from an information signal (page 1, column 1, paragraph 9 and column 2, paragraphs 18-19); and

- means for determining a matching digital fingerprint from the plurality of digital reference fingerprints as corresponding to the calculated digital fingerprint (page 2, column 1, paragraph 25); but does not specifically teach where each digital fingerprint is associated with a corresponding watermark secret; or

- means for detecting whether a digital watermark according to the watermark secret associated with the matching digital fingerprint is present in the information signal.

However, Depovere teaches where each digital fingerprint is associated with a corresponding watermark secret (page 427, column 1 and Fig. 1); and

- means for detecting whether a digital watermark according to the watermark secret associated with the matching digital fingerprint is present in the information signal (page 427, column 1 and Fig. 1 and page 428, column 2).

Response to Arguments

11. Applicant's arguments, with regards to claims 1-16 filed December 3, 2008 have been fully considered but they are not persuasive.

12. On pages 6-7 of the Response, Applicant argues that Conwell does not teach, show, or suggest "wherein the identifier data item identifying the information signal by a function which is computationally hard or infeasible to invert is used for deriving the watermark secret."

13. The Examiner points at that this argument is moot in that the limitations are amended additions to claim 1 which were originally presented in claim 4, and as such are taught by Chang as in the previous Office Action and as repeated and expanded upon in the rejection for claim 1 above.

14. On pages 6-7 of the Response, Applicant further argues that Conwell does not teach, show, or suggest "storing, in relation to the reference digital fingerprint, said identifier item."

15. The Examiner respectfully disagrees with this argument, because, as expanded on above, Conwell explicitly shows storing in the database stores the one or more songs (e.g. a song title being the identifier data item) which match the fingerprint in the database (i.e. is stored in relation to the fingerprint).

16. On page 7 of the Response, Applicant argues that there is no motivation to combine Depovere and Conwell, and in particular "Depovere is only concerned with improving the security of watermark systems."

17. In response to Applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the

references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988)and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, the cited portion of Depovere (page 429, column 1, first paragraph) states "in order to not increase the complexity of the watermark detection by a large factor it is necessary that the robust signature, and thus the secret key, does change slowly over time. Of course, the embedder and detector should be able to store the secret key patterns" Depovere's "robust signature" and corresponding "secret key patterns" utilize the same properties and are thus substantially the same as Conwell's "fingerprints." The motivation to combine is the ease of use provided by these fingerprints in data retrieval, in general (as in Conwell) and for the particular purpose of security (watermark embedding/detection as in Depovere).

18. On pages 8-9 of the Response, the Applicant argues that neither Conwell nor Depovere teach, show or suggest "detecting whether a digital watermark according to the watermark secret associated with the matching digital fingerprint is present in the information signal," and in particular "Depovere only appears to remove the embedded watermark and recover the payload, P_1".

19. The Examiner wishes to call attention to page Depovere, page 427, column 2, which states "the watermark embedder should contain a built-in watermark detector which prevents the embedding of a particular payload into content that has already been watermarked, using the same secret key" and further down "[e]ach watermark detector should be able to detect the payload embedded by any of the embedders,"

both of which necessarily requires that the detector be able to detect the presence of the watermark secret. Furthermore, even if the Applicant were correct about the function of Depovere's detectors, the attempted extraction of the payload contained in a watermarked signal and the corresponding presence or absence of the expected payload also serves as a means of detecting the watermark signal containing said payload.

20. Therefore, in view of the above reasons, Examiner maintains the rejections.

Conclusion

21. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Travis Pogmore whose telephone number is (571)270-

7313. The examiner can normally be reached on Monday through Thursday between 8:30 a.m. and 4:00 p.m. eastern time.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Thomas Pham can be reached on 571-272-3689. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/T. P./
Examiner, Art Unit 2436

/Thomas K Pham/
Supervisory Patent Examiner, Art Unit 4148